CLAIMS

What is claimed is:

1. A system for accessing multiple different network stations without entry of a password, comprising:

a first network station representing a network entity and configured to transmit a request for authentication of a user seeking access, the user having an associated password, an associated user identifier, and an associated asymmetric crypto-key, including a first private key portion obtainable with the password, a second private key portion and a public key portion;

a second network station representing the user, and having the user identifier, a combination symmetric crypto-key corresponding to a first symmetric crypto-key and a second symmetric crypto-key, and the obtained first private key portion encrypted with the first symmetric crypto-key stored thereat, and configured to (i) transmit the stored user identifier MAC'd with the stored combination symmetric crypto-key responsive to the transmitted authentication request, and (ii) transmit the transmitted authentication request encrypted with the stored combination symmetric crypto-key; and

a third network station, representing a sponsor, having the user identifier, the combination symmetric crypto-key, the first symmetric crypto-key, and the second private key portion stored thereat, and configured to (i) retrieve the stored combination symmetric crypto-key by matching the transmitted user identifier with the stored user identifier, (ii) verify the MAC with the retrieved combination symmetric crypto-key to verify identity of the user, (iii) decrypt the transmitted

encrypted authentication request with the retrieved combination symmetric crypto-key to recover the authentication request, (iv) encrypt the recovered authentication request with the stored second private key portion and (v) transmit the encrypted authentication request and the first symmetric crypto-key, both encrypted with the retrieved combination symmetric crypto-key;

wherein the second network station is further configured to (i) decrypt the transmitted encrypted authentication request and first symmetric crypto-key, with the stored combination symmetric crypto-key to recover the encrypted authentication request and the first symmetric crypto-key, (ii) decrypt the stored encrypted first private key portion with the recovered first symmetric crypto-key to recover the first private key portion, (iii) to transmit the recovered encrypted authentication request further encrypted with the recovered first private key portion; and

wherein the first station is further configured to decrypt the transmitted further encrypted authentication request with the public key to thereby authenticate the user.

2. A system according to claim 1, wherein the authentication request is a hash message.

3. A system according to claim 1, wherein the second network station is further configured to receive the password as a user input and obtain the first private key portion with the input password, prior to transmission of the authorization request by the first station.

4. A system according to claim 1, wherein the combination symmetric crypto-key corresponds to the first symmetric crypto-key XOR'd with the second symmetric crypto-key.

5. A system according to claim 1, wherein the second network station is further configured to automatically respond to the authentication request without the user inputting the password.

6. A system according to claim 1, wherein the first symmetric crypto-key is a first random number having a length of 192 bits and the second symmetric crypto-key is a second random number, different than the first random number, having a length of 192 bits.

7. A system according to claim 1, wherein the third station has a time value, representing a time period for authenticating the user, stored thereat, and is further configured to retrieve the stored time value prior to encrypting the recovered authentication request and to only encrypt the recovered authentication request if the present time is within the time period represented by the time value.

8. A system according to claim 1, wherein the second network station is further configured to generate the first symmetric crypto-key, and transmit the first symmetric crypto-key encrypted with the obtained first private key portion to the third network station;

the third station is further configured to decrypt the transmitted encrypted first symmetric crypto-key with the second private key portion to recover the first

symmetric crypto-key and thereby authenticate the user, to store the decrypted first symmetric crypto-key, to generate the second symmetric crypto-key, to combine the first and the second symmetric crypto-key to form the combination symmetric crypto-key, to store the combination symmetric crypto-key, to transmit the second symmetric crypto-key encrypted with the first symmetric crypto-key to the second network station, and to destroy the second symmetric crypto-key; and

the second network station is further configured to decrypt the transmitted encrypted second symmetric crypto-key with the first symmetric crypto-key to recover the second symmetric crypto-key and thereby authenticate the sponsor, to combine the recovered second symmetric crypto-key with the first symmetric crypto-key to form the combination symmetric crypto-key, to store the combination symmetric crypto-key, to encrypt the first private key portion with the first symmetric crypto-key, to store the encrypted first private key portion, and to destroy the first symmetric crypto-key and the unencrypted first private key portion.

9. A system for accessing multiple different network stations, comprising:

a first station representing a user having a password, an identifier, and an asymmetric crypto-key, including a first private key portion, a second private key portion and a public key portion, and configured to transmit a log-in request including the user identifier; and

a second station representing a sponsor and configured to transmit a challenge responsive to the transmitted log-in request;

wherein the first station is further configured (i) to process the user password to obtain the first private key portion, (ii) to encrypt a first symmetric crypto-key and

the transmitted challenge with the obtained first private key portion to form a first encrypted message, and (iii) to transmit the first encrypted message;

wherein the second station is further configured (i) to decrypt the transmitted first encrypted message with the second private key portion to recover the challenge and the first symmetric crypto-key, thereby authenticating the user, (ii) to combine the recovered first symmetric crypto-key with a second symmetric crypto-key to form a combined symmetric crypto-key, (iii) to store the combined symmetric crypto-key, (iv) to encrypt the second symmetric crypto-key and a time value with the first symmetric crypto-key to form a second encrypted message, and (v) to transmit the second encrypted message;

wherein the first station is further configured (i) to decrypt the transmitted second encrypted message with the first symmetric crypto-key to recover the second symmetric crypto-key and the time value, thereby authenticating the sponsor, (ii) to combine the recovered second symmetric crypto-key with the first symmetric crypto-key to form the combined symmetric crypto-key, (iii) to encrypt the first private key portion with the first symmetric crypto-key, (iv) to destroy the first symmetric crypto-key and the obtained first private key portion, (v) to encrypt a request for user authentication from another network entity with the combined symmetric crypto-key to form a third encrypted message and (vi) to transmit the user identifier, MAC'd with the combined symmetric crypto-key, and the third encrypted message;

wherein the second station is further configured (i) to match the transmitted user identifier with the previously transmitted user identifier to retrieve the combined symmetric crypto-key, (ii) verify the MAC with the retrieved combined symmetric crypto-key to verify identity of the user, (iii) to decrypt the third encrypted message with the combined symmetric crypto-key to recover the request for user

authentication, (iv) to encrypt the request for user authentication with the second private key portion to form a fourth encrypted message, (v) to encrypt the first symmetric crypto-key and the fourth encrypted message with the combined symmetric crypto-key to form a fifth encrypted message and (vi) to transmit the fifth encrypted message;

wherein the first network station is further configured (i) to decrypt the transmitted fifth encrypted message with the combined symmetric crypto-key to recover the transmitted first symmetric crypto-key and the transmitted fourth encrypted message, and thereby verify an identity of the sponsor, (ii) to decrypt the encrypted first private key portion with the recovered first symmetric crypto-key, (iii) to further encrypt the recovered fourth encrypted message with the decrypted first private key portion to form an authentication message, (iv) to transmit the authentication message to the other network entity to authenticate the user.

10. A method for accessing multiple different network stations without entry of a password associated with a user also having an associated identifier and an associated asymmetric crypto-key, including a first private key portion obtainable with the password, a second private key portion and a public key portion, comprising:

receiving a request for authentication of the user;

retrieving from a first memory, without entry of the user password, the user identifier, a combination symmetric crypto-key corresponding to a first symmetric crypto-key and a second symmetric crypto-key, and the first private key portion encrypted with the first symmetric crypto-key;

encrypting the transmitted authentication request with the retrieved combination symmetric crypto-key;

transmitting the retrieved user identifier MAC'd with the retrieved combination symmetric crypto-key, and the received authentication request encrypted with the retrieved combination symmetric crypto-key;

matching the transmitted user identifier with a user identifier stored in a second memory, different than the first memory, to retrieve the combination symmetric crypto-key from the second memory;

verifying the MAC with the retrieved combination symmetric crypto-key to verify identity of the user;

decrypting the transmitted encrypted authentication request with the combination symmetric crypto-key to recover the authorization request;

retrieving the second private key portion and the first symmetric crypto-key from the second memory;

encrypting the recovered authorization request with the retrieved second private key portion to form an authentication message;

transmitting the authentication message and the retrieved first symmetric crypto-key, both encrypted with the combination symmetric crypto-key;

decrypting the transmitted encrypted authentication message and first symmetric crypto-key, with the combination symmetric crypto-key retrieved from the first memory to recover the authentication message and the first symmetric crypto-key;

decrypting the retrieved encrypted first private key portion with the recovered first symmetric crypto-key;

encrypting the recovered authentication message with the decrypted first private key portion to complete the authentication message;

transmitting the completed authentication message; and

decrypting the transmitted completed authentication message with the user public key to thereby authenticate the user.

11. A method according to claim 10, wherein the authentication request is a hash message.

12. A method according to claim 10, further comprising:

processing the user password to obtain the first private key portion, prior to receipt of the authentication request.

13. A method according to claim 10, further comprising:

XOR'ing the first symmetric crypto-key with the second symmetric crypto-key to generate the combination symmetric crypto-key.

14. A method according to claim 10, wherein the first symmetric crypto-key is a first random number having a length of 192 bits and the second symmetric crypto-key is a second random number, different than the first random number, having a length of 192 bits.

15. A method according to claim 10, further comprising:

retrieving a time value, representing a time period for authenticating the user, from the second memory; and

only encrypting the recovered authentication request if the present time is within the time period represented by the retrieved time value.

16. A method according to claim 10, further comprising:

generating the first symmetric crypto-key;

transmitting the first symmetric crypto-key encrypted with the obtained first private key portion;

decrypting the transmitted encrypted first symmetric crypto-key with the second private key portion to recover the first symmetric crypto-key and thereby authenticate the user;

storing the decrypted first symmetric crypto-key in the second memory;

generating the second symmetric crypto-key;

combining the first and the second symmetric crypto-keys to form the combination symmetric crypto-key;

storing the combination symmetric crypto-key in the second memory;

transmitting the second symmetric crypto-key encrypted with the first symmetric crypto-key;

destroying the second symmetric crypto-key;

decrypting the transmitted encrypted second symmetric crypto-key with the first symmetric crypto-key to recover the second symmetric crypto-key and thereby authenticate the sponsor;

combining the recovered second symmetric crypto-key with the first symmetric crypto-key to form the combination symmetric crypto-key;

storing the combination symmetric crypto-key in the first memory;

encrypting the first private key portion with the first symmetric crypto-key;

storing the encrypted first private key portion in the first memory; and

destroying the first symmetric crypto-key used to encrypt the first private key portion and the unencrypted first private key portion.

17. A method for accessing multiple different network stations by a user having a user identifier, a user password and an asymmetric crypto-key, including a first private key portion, a second private key portion and a public key portion;

transmitting a log-in request including the user identifier;

transmitting a challenge of a sponsor responsive to the transmitted log-in request;

processing the user password to obtain the first private key portion;

encrypting a first symmetric crypto-key and the transmitted challenge with the obtained first private key portion to form a first encrypted message;

transmitting the first encrypted message;

decrypting the transmitted first encrypted message with the second private key portion to recover the challenge and the first symmetric crypto-key, and thereby authenticate the user to the sponsor;

combining the recovered first symmetric crypto-key with a second symmetric crypto-key to form a combined symmetric crypto-key;

storing the combined symmetric crypto-key in a first memory;

encrypting the second symmetric crypto-key with the first symmetric crypto-key to form a second encrypted message;

transmitting the second encrypted message;

decrypting the transmitted second encrypted message with the first symmetric crypto-key to recover the second symmetric crypto-key, and thereby authenticate the sponsor to the user;

combining the recovered second symmetric crypto-key with the first symmetric crypto-key to form the combined symmetric crypto-key;

storing the combined symmetric crypto-key in a second memory, different than the first memory;

encrypting the first private key portion with the first symmetric crypto-key;

destroying the first symmetric crypto-key used to encrypt the first private key portion and the obtained first private key portion;

encrypting a request for authentication of the user with the combined symmetric crypto-key to form a third encrypted message;

transmitting the user identifier, MAC'd with the combined symmetric crypto-key, and the third encrypted message;

matching the transmitted user identifier with the previously transmitted user identifier to retrieve the combined symmetric crypto-key from the second memory;

verifying the transmitted MAC with the retrieved combined symmetric crypto-key to verify an identity of the user;

decrypting the third encrypted message with the combined symmetric crypto-key to recover the request for user authentication;

encrypting the request for user authentication with the second private key portion to form a fourth encrypted message;

encrypting the first symmetric crypto-key and the fourth encrypted message with the combined symmetric crypto-key stored in the first memory to form a fifth encrypted message;

transmitting the fifth encrypted message;

decrypting the transmitted fifth encrypted message with the combined symmetric crypto-key stored in the second memory to recover the transmitted first symmetric crypto-key and the transmitted fourth encrypted message, and thereby verify an identity of the sponsor;

decrypting the encrypted first private key portion with the recovered first symmetric crypto-key;

further encrypting the recovered fourth encrypted message with the decrypted first private key portion to form an authentication message;

transmitting the authentication message to the other network entity to authenticate the user.

18. A method for accessing multiple different network stations without entry of a password associated with a user having an associated first symmetric crypto-key, an associated second symmetric crypto-key and an associated asymmetric crypto-key, including a first private key portion, a second private key portion and a public key portion, comprising:

encrypting the first private key portion with the first symmetric crypto-key;

transmitting a request, of a network station, for authentication of the user, encrypted with the second symmetric crypto-key to a sponsor;

decrypting the transmitted encrypted authentication request with the second symmetric crypto-key to recover the authentication request;

encrypting the recovered authentication request with the second private key portion to form an authentication message;

transmitting the authentication message and the first symmetric crypto-key, both encrypted with the second symmetric crypto-key to the user;

decrypting both the transmitted encrypted authentication message and the transmitted encrypted first symmetric crypto-key with the second symmetric crypto-key to recover the authentication message and the first symmetric crypto-key;

decrypting the first private key portion with the recovered first symmetric crypto-key;

transmitting the authentication message encrypted the recovered first symmetric crypto-key to the network station; and

decrypting the transmitted encrypted authentication message with the public key portion to recover the authentication request and thereby authenticate the user to the network station.